FICAS SECURITY MODULE MAINTENANCE INSTRUCTIONS

Overview

The FICAS security module allows administrators to manage users and their access to site data and functionality. The security module determines user access to system features at the agency, user type, and user identification levels. Users may or may not be permitted to inquire into or update system files and tables.

Users are required to attend a VFA certification training prior to gaining access to the FICAS System.

Policy

The security module is currently controlled by VFA. The Auditor of Public Accounts approves all system users and changes that VFA completes in the security module. It is the responsibility of each agency's FICAS Security Officer to ensure that adequate internal controls exist within that agency to prevent unauthorized access to online FICAS data, and that each logon ID (identification number) is assigned to an individual, not to a group or section.

FICAS Security Officer

Each agency head is responsible for designating an individual as the FICAS Security Officer. In addition, each agency head will serve as an ex officio FICAS Security Officer.

Duties of the FICAS Security Officer

The primary purpose of the FICAS Security Officer is to control, within APA constraints, an agency's access to FICAS by its personnel. In addition, this position serves as the key liaison between APA and all agency personnel who interact with FICAS, submit data to FICAS, and hold an interest in FICAS reports. The FICAS Security Officer is responsible for the following at a minimum.

- Maintenance of a comprehensive intra-agency system of internal control over both online and offline access to FICAS tables and files, within the constraints described in this section.

- Maintenance of a current mailing address on the APA mailing list, "FICAS Security Officers." Requests for additions or changes to the APA mailing list for FICAS Security Officers must meet the following specifications.

  Address: **U. S. Mail**
  Katie Collins, FICAS Project Manager
  Auditor of Public Accounts
  Post Office Box 1295
  Richmond, VA 23218

Other Delivery:

Katie Collins, FICAS Project Manager
Auditor of Public Accounts
8th Floor, Monroe Building
101 North 14th Street
Richmond, VA 23219

Format: Request must be typed on agency letterhead.

Authorization: Must be signed in full by FICAS Security Officer.

Data Required: Agency Name and Number
FICAS Name and Signature
Agencies for which the Change is Effective
Effective Date
Mailing Address

- Receipt and dissemination of documentation to all agency operating personnel requiring FICAS policies and procedures.

- Notation of the FICAS Security Officer will be accomplished by completing the FICAS Security Module Maintenance Form on APA's website (www.apa.virginia.gov/deferred_maintenance.htm). This form should be completed and submitted to FICAS@apa.virginia.gov. Due to the critical nature of the Security Officer function and the need to maintain continuity in agency FICAS operation, APA requires the naming of a FICAS Security Officer on the individual's Security Form. Also, the agency head is empowered to act as a FICAS Security Officer, whether or not Security Officer designation appears on the Security Form.

  LIMITATION: One designated Security Officer per agency number, not including the agency head.

Security Officer Scope of Authority

The FICAS Security Officer may authorize access, within APA constraints, to FICAS, for the agency number that corresponds to the FICAS Security Module Maintenance Form designating Security Officer status. However, if a control agency's signature card designates Security Officer status, that status is valid for that control agency as well as any "controlled" agencies. Control/controlled agency relationships are defined by CAPP Manual Topic No. 60104, "Agency and FIPS Codes."

FICAS Security Module Maintenance Form (FICAS Access Form)

An electronic copy of this form can be located on the Auditor of Public Account's website at www.apa.virginia.gov using the link FICAS – Deferred Maintenance.

Follow the procedures below when submitting FICAS Security Module Maintenance Forms to APA for entry to FICAS. Instructions are provided for each of the major components of the Access Form including the:

- User Identification
- Function
- Role
- Data View
- Assets
- Projects - Plan Group
- Cost Model Group

User Identification Elements

The five elements which identify each user on the Security Form are the User Name, User Phone Number, User Title/Job Responsibilities, User Email Address, and User Agency.

User Name

USER NAME is a field that contains the user's English name.

User Phone Number

USER PHONE NUMBER is a field that contains the user's telephone number at which they can be reached.

User Title/Job Responsibilities

USER TITLE/JOB RESPONSIBILITIES is a field that identifies why the user needs access to the system based on their job requirements.

User Email Address

USER EMAIL ADDRESS is a field that contains the user's full state email address. An agency can not obtain access for a user without an e-mail address. This e-mail must belong to the designated user.

User Agency

The USER AGENCY is a field that identifies the state agency with which the user is associated.

Function

The function codes used to update the FICAS Security Module are:
Add = Add a new user ID to the system
Change = Change user ID in the system
Delete = Delete user ID from the system

Role

The ROLE component of the FICAS Security Form includes four access possibilities (Administrator, Assessor, Manager, or Planner).

- Administrator has rights to the entire vaficas.vfafacility.com site. APA is the only agency at this time with these rights.

- Assessor has access to view and use data for their agency only. Within their agency, assessor users have create and edit access to the Asset Module, read-only access to the Projects Module, and read only access to Cost Modules.
- Manager has access to view and use data for their agency only. Within their agency, managers have create and edit access to the Asset Module, full access (create, edit, and delete) to Projects Module, and full access to Cost Models.
- Planner currently is defined the same as Manager.

Data View

The DATA VIEW component of the FICAS Security Form includes two view possibilities (Statewide or Agency). Most individuals will have agency view access. The Statewide view access only applies to the Department of Planning and Budget and Department of General Services. The State Council for Higher Education of Virginia may acquire access for all colleges and universities.

Assets

The ASSETS component of the FICAS Security Form includes four access possibilities (Full, Create, Edit, and Read-only). See Appendix A for additional explanation of Full, Create, Edit, and Read-only.

Projects

The PROJECTS component of the FICAS Security Form includes two access possibilities (Full and Read-only). See Appendix A for additional explanation of Full and Read-only.

Cost Models

The COST MODELS component of the FICAS Security Form includes two access possibilities (Full and Read-only). See Appendix A for additional explanation of Full and Read-only.

APA Control Restrictions

APA will review each of the FICAS Security Module Maintenance Forms for approval. Incorrectly prepared FICAS Security Forms will be returned to the agency. APA will not correct any errors or omissions on the form.

1. The form must be typed or legibly printed in ink.
2. No erasures, correction fluid, correction tape, or other alterations may appear on the FICAS Security Form.
3. For any changes to a given user ID on the FICAS Security Form, only the data to be changed should be entered on the Form.
4. The original copy of the form must be submitted to the APA.

APA Submission

Date: 2/1/06

Upon completion of the FICAS Security Module Maintenance Form, agencies are required to submit the form to the APA. This form can be submitted via fax (804-786-5593 Attention: Katie Collins, FICAS Project Manager) or email (FICAS@apa.virginia.gov) to expedite the process of obtaining access to the system. But the original copy of the access form must be mailed to the APA at: Auditor of Public Accounts; Attention: Katie Collins, FICAS Project Manager; P.O. Box 1295; Richmond, VA 23218. Upon completion of the addition, deletions or changes, APA will return a confirmation copy to the agency. Please review this copy to ensure that the changes made to the security table record are as you intended. If an error is noted on the security form, a new form must be completed and resubmitted to APA.

Internal Control

The control of an agency's access to FICAS is vital. The FICAS Security Officer is responsible for a comprehensive system of internal control over both on-line and off-line access to FICAS tables and files. This access control is vital to ensure the integrity of transactions submitted to FICAS.

Users should ensure that they are not sharing user identifications and passwords. This information is user specific.

Records Retention

Security Table Maintenance Forms must be retained for three (3) years or until audited by the Auditor of Public Accounts, whichever is longer.

APA Contacts

Katie Collins, FICAS Project Manager, 804-225-3350; Katherine.Collins@apa.virginia.gov

DeAnn Compton, FICAS Project Director, 804-225-3350 ext. 344;
DeAnn.Compton@apa.virginia.gov

References

VFA.facility 6.1.4 Administration Guide

FICAS System Application – Security Manual

Appendix A

Reference: *VFA.facility 6.1.4 Administration Guide*

Part 1: Security Module

Assets

Task ↓	Full Access	Create*	Edit	Read-Only	No Access
View asset?	Yes	Yes	Yes	Yes	No
Edit asset fields?	Yes	Yes	Yes	No	No
Copy asset?	Yes	Yes	Yes	Yes	No
Paste asset? (permission needed for the campus)	Yes	Yes	No	No	No
Move asset? (permission needed for the asset)	Yes	No	No	No	No
Move asset? (permission needed for the campus)	Yes	Yes	No	No	No
Delete asset?	Yes	No	No	No	No
Create asset?	Yes	Yes	No	No	No
Create, modify, link and delete asset subordinate?**	Yes	Yes	Yes	No	No

** Users have Full Access to the assets that they create until the privilege is changed.*

*** Asset subordinates include rooms, assemblies, requirements, actions, photos and CAD drawings.*

Project Groups

To access the Projects module, a user needs the Project Planning capability. See *About Capabilities* on page 10.

Task ↓	Full Access	Create	Edit	Read-Only	No Access
View project group?	Yes	Yes	Yes	Yes	No
Edit project group fields?	Yes	Yes	Yes	No	No
Add a project to a plan in project group?	Yes	Yes	Yes	No	No
Delete a project from a plan in a project group?	Yes	Yes	Yes	No	No
Create projects and plans in project group?	Yes	Yes	No	No	No
Edit projects and plans in project group? **	Yes	Yes	Yes	No	No
Delete projects and plans in project group? **	Yes	No*	No	No	No
Copy project in project group?	Yes	Yes	Yes	Yes	No
Paste project in project group? (permission needed for project group)	Yes	Yes	No	No	No
Move project? (permission needed for the project group)	Yes	Yes	No	No	No

Task ↓	Full Access	Create	Edit	Read-Only	No Access
Move project? (permission needed for project)	Yes	No*	No	No	No
Add requirement to project?	User needs at least Read-Only access to the asset, and at least Edit access to the project group.				
Create project group?	User needs at least default Create access to project groups.				
Copy/Paste project group?	User needs at least default Create access to project groups.				
Delete project group?	User needs at least default Full access to project groups.				

** A user has Full Access to projects and plans that they create until the privilege is changed.*

*** When working in a fiscal plan's Project Calendar, a user with access to the fiscal plan can view and work with any projects in that plan, including projects added from other project groups that the user may not have access privileges to.*

Cost Model Groups

Task ↓	Full Access	Read-Only Access
View cost model?	Yes	Yes
Assign cost model to asset?	Yes	Yes
Edit cost model fields?	Yes	No
Delete cost model?	Yes	No
Create cost model?	Yes	No
Copy cost model?	Yes	No
Create cost model group?	Only Administrators can create cost model groups.	
Delete cost model group?	Only Administrators can delete cost model groups.	

Reports and Forecasts

When a user generates a report, funding analysis, or Data Browser query, it will not contain data that a user has **No Access to**.